UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/730,183	12/08/2003	Herbert A. Little	555255012471	2882

7590 02/07/2007

David B. Cochran, Esq.
JONES DAY
North Point
901 Lakeside Ave
Cleveland, OH 44114

EXAMINER	
ZEE, EDWARD	
ART UNIT	**PAPER NUMBER**
2109	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	02/07/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	Application No.	Applicant(s)	
	10/730,183	LITTLE ET AL.	
	Examiner	Art Unit	
	Edward Zee	2109	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *08 December 2003*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *08 December 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *06/16/04, 05/25/06*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This action is in response to the original filing of December 8, 2003. Claims 1-32 are pending and have been considered below.

Specification

2. The disclosure is objected to because of the following informalities: the examiner notes the use of acronyms (ie. PC, WAP, RAM, AMPS, PIM, etc.) throughout the specification without first including a description in plain text, as required. There also appears to be a typographical error in page 25, line 21-22 of the specification; "two-factor code generator" is labeled as object 202, however in the figure it is labeled as object 210.

Appropriate correction is required.

3. The use of the trademarks Bluetooth®, Microsoft Outlook® and Lotus Notes® has been noted in this application. It should be capitalized wherever it appears and be accompanied by the generic terminology.

Although the use of trademarks is permissible in patent applications, the proprietary nature of the marks should be respected and every effort made to prevent their use in any manner which might adversely affect their validity as trademarks.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. Claims 1-3, 7, 8, 11-15, 18, 20, 23 and 29 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1, 2, 7, 8, 18 and 23: The terms "for use", "to be used", "allows" and "enables" in claims 1, 2, 7, 8, 18 and 23 render the claims indefinite.

Claim 3: The examiner notes that the language in claim 3 is unclear and the applicant appears to claim sending the seed value, originally sent by the remote device to the authentication system, from the authentication system back to the remote device. There will be little or no patentable weight given to this step.

Claims 11 and 12: The term "normally not known to the user of a remote device" in claims 11 and 12 render the claims indefinite. The examiner notes that this can be interpreted as "normally not known but can be known to the user of a remote device" and will examine the claims in this manner.

Claim 13-15: The term "relatively short" in claims 13-15 is a relative term which renders the claims indefinite. The term "relatively short" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. The examiner notes that the term "order of minutes" fails to further define the degree of "relatively short". The examiner will give little or no patentable weight to this term while examining the claims below.

Claim 20: The term "for use by the remote device's two-factor code generator" in claim 20 renders the claim indefinite. The examiner will give little or no patentable weight to this term while examining the claim below.

Claim 29: The term "includes a wide area network(WAN) and a wireless network gateway" in claim 29 renders the claim indefinite. The examiner notes this can be interpreted as "includes but not limited to a wide area network(WAN) and a wireless network gateway" and will examine the claim in this manner.

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 30 and 32 are rejected under 35 U.S.C. 102(b) as being anticipated by Guthrie et al. (6,161,185).

Claim 30: Guthrie et al. discloses a method for distributing authentication information for remotely accessing computer resources, comprising:

a. receiving a request for the authentication information from a remote device*(client transmits user account and password to the server)*, the request comprising identity information of a user*(user inputs user account and password)* of the remote device [column 7, lines 14-19];

b. authenticating the user based on the identity information*(validates the user account and password against the user's account table stored in the user account database)* in the request [column 7, lines 19-21];

c. returning the authentication information to the remote device so that the remote device*(transmits the challenge to the client)* may access the computer resources based upon the

returned authentication information*(The server provides the client with a message indicating whether the authentication succeeded or failed, and enables appropriate access if successful)* [column 7, lines 22-26 & 41-44].

Claim 32: Guthrie et al. discloses a method for obtaining authentication information for remotely accessing a computer network, comprising:

a. providing a request from a user of a remote device to an authentication system for the authentication information*(client transmits user account and password to the server)* [column 7, lines 14-19];

b. the request includes identity information*(user inputs user account and password)* for use by the authentication system to authenticate the user based on the identity information*(validates the user account and password against the user's account table stored in the user account database)* provided in the request [column 7, lines 14-21];

c. receiving by the remote device the authentication information from the authentication system*(transmits the challenge to the client)* [column 7, lines 22-26];

e. the received authentication information*(challenge)* is to be used by the remote device*(client uses challenge to generate a response and transmits it to the server)* to access the computer network*(the server provides the client with a message indicating whether the authentication succeeded or failed, and enables appropriate access if successful)* [column 7, lines 29-45].

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-19, 24-29 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthrie et al. (6,161,185).

Claim 1: Guthrie et al. discloses a system for distributing authentication information to users of remote devices comprising:

a. an authentication information store*(user account database)* configured to store authentication information for a plurality of users*(database includes tables of users accounts, including account IDs)* [column 5, lines 35-42];

b. an authentication system configured to receive a request for authentication information*(user provides an account identifier and corresponding account password to initially log on to or access the server)* for one of the plurality of users from a remote device*(client computer)* [column 4, lines 3-16];

c. wherein the request includes identity information*(account identifier)* for use in determining whether the request is from one of the plurality of users*(compares the received user account ID to a user account table)* [column 4, lines 3-5 & column 8, lines 1-2];

d. wherein the authentication system retrieves based on the identity information*(user account ID)* the authentication information*(user account table)* for the one of the plurality of users from the authentication information store*(user account database)* [column 7, lines 64-66];

However, Guthrie et al. does not explicitly disclose that the retrieved authentication information is provided to the remote device. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to send the authentication information back to the remote device. One would have been motivated to do so in order to conserve processor resources on the server by sending the authentication information to the remote device and performing the authentication process locally on the remote device.

Claim 2: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information is used in a two-factor authentication system [column 4, lines 1-8].

Claim 3: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information store*(account user database)* includes a seed store configured to store a plurality of seeds*(the serial number and SADB password are stored in the user's account table in the user account database)*, wherein the authentication system is configured to receive a seed request*(the client then transmits the response produced by the client SADB calculator to the server)*, including an access code generated using one of the plurality of seeds*(the client calculator generates the response using the challenge, SADB password and the locally stored serial number)*, from the remote device, to retrieve the one of the plurality of seeds from the seed store, to calculate an access code using the retrieved seed*(using the same serial number, SADB password and challenge, both the client and server SADB calculators should produce the same response)*, to determine whether the calculated access code matches the received access code*(the server compares its internally generated response with the response received by the client)*, but does

not explicitly disclose that the retrieved seed is returned to the remote device if the access code matches the received access code [column 6, lines 65-67 & column 7, lines 1-9]. However, it would have been obvious to one of ordinary skill in the art at the time of invention to return the retrieved see to the remote device. One would have been motivated to do so in order to establish a successful authentication and to ensure that the seed value is not used again. This would provide enhanced security in the authentication system.

Claim 4: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above but does not explicitly disclose that the request comprises a Hypertext Transfer Protocol(HTTP) connection request. However, Guthrie et al. discloses that the server includes a TCP/IP based web server that provides to the client several hypertext markup language(HTML) pages or other displayable screens to the user so that the client can interact with the server via several HTML pages [column 14, lines 4-13]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to use an HTTP connection for displaying HTML pages.

Claim 5: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the request includes a network password*(account password)* and a digital signature*(response generated with secured hashing algorithm)*, but does not explicitly disclose that the network password and digital signature are verified by the authentication system before the authentication information is provided to the remote device [column 6, lines 14-17]. However, it would have been obvious to one of ordinary skill in the art at the time of invention that one would first verify the user before sending

authentication information back to the remote device. One would be motivated to do so in order to maintain a higher level of security within the system.

Claim 6: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the identity information*(user account ID)* includes user information and account information*(associated with a number of designations or code indicating that the account corresponds to that of a system administrator or other account having high priorities)* [column 7, lines 54-59].

Claim 7: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 6 above and further discloses that the identity information*(user account ID)* identifies a particular user and corresponding authentication information being requested*(the server retrieves the corresponding user account table in the user account database which corresponds to the user account ID)*, and allows the authentication system to authenticate the user requesting the authentication information*(the server retrieves a user account table and compares the received user account ID to the user account ID data record)* [column 7, lines 64-67 & column 8, lines 1-2].

Claim 8: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information enables two-factor authentication at the computer network [column 4, lines 1-8].

Claim 9: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 8 above and further discloses that the identity information includes a network password*(user password)* entered by the user of the remote device and a digital signature generated based on a transformation of at least a portion of the information in the

request, a signature key*(serial number)*, and a signature algorithm*(SADB password and challenge data input together with the serial number to a secure hashing algorithm)* [column 6, lines 14-17].

Claim 10: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication system does not provide the authentication information to the remote device because a match was not found in the authentication information store based upon the identity information [Figure 7A]. The examiner notes that ending the process if a match is not found is equivalent to not providing the authentication information to the remote device.

Claim 11: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the authentication information includes a password*(SADB password)* which is required for remote access to resources in the computer network*(the server provides the client with a message indicating whether the authentication succeeded or failed, and enables appropriate access if successful)* [column 15, lines 53-57 & column 7, lines 29-45].

Claim 12: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses an access code*(response)* which is required for remote access to resources in the computer network*(the server provides the client with a message indication whether the authentication succeeded or failed, and enables appropriate access if successful)*, but does not explicitly disclose that the access code is contained within the authentication information [column 7, lines 10-44]. However, it would have been obvious to one of ordinary skill in the art at the time of invention to include the access

code in the authentication information or any other information that is required for authentication. One would have been motivated to do so in order to verify that the access has been granted to the user.

Claims 13-16: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the retrieved authentication information includes an expiring password*(account passwords expire after a select period of time, typically a few weeks)* and access code*(the response generated by the client's calculator is invalid after a short period of time)* [column 4, lines 35-39]. However, Guthrie et al. does not explicitly disclose that the passwords can be set to not expire and that the password is stored in a protected data store on the remote device. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to set the passwords to not expire. One would have been motivated to do so in order to reduce the amount of lost passwords amongst the users. Official Notice is taken that it is old and well known within the cryptographic arts to store frequently used passwords in a protected database on the remote device. For example, the Microsoft Internet Explorer® web browser offers it's user the option of storing a password in a protected database, located in the user's local disc drive, when logging into a password protected website. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to store the password in a protected data store on the remote device.

Claim 17: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the retrieved authentication information includes a seed*(serial number)* from which access codes are to be generated by the remote device, wherein the seed is stored on the remote device*(the serial number is stored*

internally in the client SADB calculator), but does not explicitly disclose that the seed is stored in a protected data store [column 5, lines 64-67]. However, it would have been obvious to one of ordinary skill in the art to store the seed in a protected data store. One would have been motivated to do so in order to prevent the seed from being compromised.

Claim 18: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the retrieved authentication information is for use by the remote device to gain access*(the present invention authenticates a user of the client to permit the user access to the server, as well as access to any resources on the server)* to a corporate local area network(LAN)*(the present invention includes an internal network coupled to the server. The internal network may be a corporate internal network, such as corporate intranet. Additionally, network resources are coupled to the server.)* [column 4, lines 60-64 & column 5, lines 7-12].

Claim 19: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 18 above and further discloses that two-factor authentication is used in the LAN to authenticate a user requesting remote access to the LAN, wherein the retrieved authentication information is used in performing two-factor authentication in order to gain access to the LAN [column 4, lines 1-8].

Claim 24: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the user may use a mobile communication device*(palm top computer)* to access the server, but does not explicitly disclose that the mobile device is wireless [column 6, lines 1-3]. However, it would have been obvious to one of ordinary skill in the art at the time of invention to use a wireless mobile communication

device. One would have been motivated to do so in order to increase the portability of the mobile device.

Claim 25: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 24 above and further discloses that the remote device*(client)* stores the authentication information*(serial number)* in a data store*(client computer downloads of copy of the SADB calculator and the serial number is stored internally in the client SADB calculator)* [column 5, lines 48-67].

Claims 26 and 27: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 25 above, but does not explicitly disclose how the data store is implemented. However, it would have been obvious to one of ordinary skill in the art at the time of invention to implement the data store on either a smart card or USB token or any other form of data storage. One would have been motivated to use either form of data storage depending on the constraints of the remote device.

Claim 28: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device is a desktop computer [column 3, lines 53-55].

Claim 29: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 1 above and further discloses that the remote device communicates with the authentication system over a communication system [column 4, lines 65-66].

Claim 31: Guthrie et al. discloses an apparatus for handling authentication information for users of remote devices, comprising:

a. an authentication information store*(user account database)* configured to store authentication information for a user of a remote device*(database includes tables of users accounts, including account IDs)*, the authentication information provided by a remote authentication system*(the user receives a user account ID and receives an account password)* [column 5, lines 35-47];

b. a request from the remote device*(client computer)* to the remote authentication system contains identity information*(user provides an account identifier and corresponding account password to initially log on to or access the server)* [column 4, lines 3-16];

c. a code generation system*(SADB calculator)* configured to retrieve the authentication information*(initial data includes a serial number and SADB password)* stored in the authentication information store*(the serial number and SADB password are stored in the user's account table in the user account database)* [column 6, lines 14-20 & lines 65-67];

d. access information is generated based upon the retrieved authentication information and is used in accessing a remote computer network*(By employing the serial number, SADB password and challenge, the SHA generates a unique response)* [column 6, lines 21-23]. However, Guthrie et al. does not explicitly disclose that the retrieved authentication information is provided to the remote device. Nonetheless, it would have been obvious to one of ordinary skill in the art at the time of invention to send the authentication information back to the remote device. One would have been motivated to do so in order to conserve processor resources on the server by sending the authentication information to the remote device and performing the authentication process locally on the remote device.

10. Claims 20-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Guthrie et al. (6,161,185) in view of Hashiguchi (6,615,353).

Claim 20: Guthrie et al. discloses a system for distributing authentication information to users of remote devices as in claim 19 above and further discloses that the retrieved authentication information includes a seed*(the serial number and SADB password are stored in the user's account table in the user account database)* used to produce an access code*(using the same serial number, SADB password and challenge, both the client and server SADB calculators should produce the same response)*, wherein the access code*(response)* is used by the remote device to gain access to the LAN; wherein the seed is used by the authentication system*(server)* to also generate an access code for use in comparison with the access code generated by the remote device; wherein the access to the LAN is granted based upon the comparison*(the server provides the client with a message indicating whether the authentication succeeded or failed, and enables the appropriate access if successful)*, but does not disclose that the access code is also based upon a value provided by the remote device's clock [column 6, lines 65-67 & column 7, lines 1-9 & column 7, lines 41-44]. However, Hashiguchi discloses a similar system for distributing authentication information to users of remote devices that further discloses the access code*(authentication code)* is based upon a value provided by the remote device's clock*(authentication code is generated using parameters stored on the floppy disk which include a date and time of the last access by the client)* [column 4, lines 11-29]. Therefore, it would have been obvious to one of ordinary skill in the art at the time of invention to base the access code off a clock value of the remote device in the system disclosed by Guthrie et al. One would have

been motivated to include the clock value in order to increase the level of security with in the authentication system.

Claim 21: Guthrie et al. and Hashiguchi disclose a system for distributing authentication information to users of remote devices as in claim 20 above and Guthrie et al. further discloses that after the user of the remote device*(client)* initiates a request for access to the LAN, the authentication system*(server)* sends a challenge to the remote device, wherein the remote device responds by generating an access code*(response)* and sends it back to the authentication system*(server)* [column 7, lines 10-45]. While it is not explicitly disclosed that the remote device only generates the access code when access to the LAN is requested, it would have been obvious. One would have been motivated to so do to preclude storing access codes on the remote device, thus decreasing the chance of compromise.

Claim 22: Guthrie et al. and Hashiguchi disclose a system for distributing authentication information to users of remote devices as in claim 20 above and Guthrie et al. further discloses that the authentication information store*(user account database)* includes an index by user name*(includes tables of users accounts, including account IDs)* that indicates users authorized for remote access to the LAN [column 5, lines 35-37]. The examiner notes that it is inherent the index of user names indicate users who are authorized for remote access.

Claim 23: Guthrie et al. and Hashiguchi disclose a system for distributing authentication information to users of remote devices as in claim 22 above and Guthrie et al. further discloses that the retrieved authentication information includes a seed*(serial number)* from which access codes*(response)* are to be generated*(using the serial number, SADB password and challenge,*

both the client and server SADB calculators should produce the same response) [column 5, lines 64-67 & column 7, lines 1-3].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Edward Zee whose telephone number is (571) 270-1686. The examiner can normally be reached on Monday through Thursday 6:30AM-5:00PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, James W. Myhre can be reached on (571) 270-1065. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

EZ
February 2, 2007

James W. Myhre
Supervisory Patent Examiner